2024-25 DCIG TOP 5

SUB-2PB+ CYBER SECURE BACKUP TARGETS // GLOBAL EDITION

By DCIG Principal Data Protection Analyst, Jerome M Wendt

Sub-2PB+ Cyber Secure Backup Targets // Global Edition

Table of Contents

Sub-2PB+ Cyber Secure Backup Targets // Global Edition

SOLUTIONS EVALUATED

1. Arcserve OneXafe 4500
2. Dell PowerProtect DD6900
3. ExaGrid EX10
4. ExaGrid EX18
5. HPE StoreOnce 3660
6. HPE StoreOnce 5660
7. Huawei OceanProtect X6000
8. iXsystems TrueNAS M30
9. iXsystems TrueNAS R20
10. iXsystems TrueNAS X20
11. Nimbus Data ExaFlash One
12. Quantum DXi4800
13. Starwind Software SA-2AF

CYBER SECURE BACKUP TARGET FEATURES EVALUATED

- API/network protocols supported.
- Data protection.
- Hardware configuration.
- Management.
- Technical support.

Cyber Security Becomes Core Backup Target Feature

Organizations have historically measured backup targets based on how well they minimally deliver on the following three features:

- Backup throughput speeds.
- Data reduction.
- Economical storage.

Ransomware threats and attacks have forced organizations to add at least one more core feature to this list: cyber security.

Organizations and managed service and technology providers now regularly report that many ransomware stains routinely target their backup infrastructures. Some ransomware strains even start their attacks by seeking to compromise or disable backup targets. They do so in one or more of the following ways:

- Compromise or obtain administrative logins to these systems.
- Delete backups residing on them.
- Encrypt backups residing on them.
- Exfiltrate, or copy, backups from the system to the hacker's site.

The Incentive for Hackers to First Attack Backup Targets

Ransomware first attacking backup targets hinders an organization's ability to recover from an attack. Having compromised the backup target in any of these ways, the ransomware then turns to attacking production IT data and systems. If it then succeeds in these attacks in production, organizations may find themselves without any restoration or recovery options.

Further adding to the danger of ransomware attacks, 90 percent of these attacks exfiltrate data.[1] Hackers may use exfiltrated data as another means to extract a ransom. Alternatively, hackers may sell the data to third parties, release it publicly, or take all these actions. Further complicating matters, organizations may lack clarity into how hackers accessed their IT infrastructure and the data they stole.[2]

Hackers may also attempt to obtain a backup target's administrative logins and passwords. If they log into the backup target with administrative permissions, a hacker may perform any number of nefarious activities. These can range from deleting backups to copying them offsite to changing file permissions and backup retention periods.

Finally, even should the backup target repel a ransomware attack, the ransomware may still compromise production systems and data. In this scenario, organizations may need the backup target to assume additional roles. These can include performing instant restores and hosting recoveries even as the solution continues functioning as a backup target.

Repelling these different attack types and assuming broader recovery capabilities demands that organizations choose cyber secure backup targets. These backup targets still deliver on the core three features that organizations expect backup targets to possess. However, cyber security features have become prerequisites for organizations seeking to protect their backups and facilitate fast restores and recoveries.

The State of Cyber Secure Backup Targets

Only recently have storage providers, as a group, begun positioning their network attached storage (NAS) solutions as backup targets. Prior to that, few storage providers formally marketed their NAS systems as backup targets. While NAS systems could serve in this role, providers downplayed this functionality.

Today, few providers exhibit any concerns about their NAS solutions being used as backup targets. More than 20 different storage providers promote more than 100 production storage systems on their respective websites as backup targets.

This report focuses on solutions that offer file protocol support.

While many of these storage systems support multiple storage protocols, this report focuses on solutions with file protocol support. These support either the Network File System (NFS), the Common Internet File System (CIFS), or both. These NAS solutions provide the following benefits for backup that organizations frequently want:

- Backup software can easily discover and utilize these solutions as backup targets.
- Client-side software available to accelerate backup throughput.
- Facilitate fast application, and data, restores.
- Fast, easy deployment, setup, and management in organizational backup infrastructures.
- Readily recognized as a storage target by all commonly used operating systems.
- Utilize standard, cost-effective Ethernet for network connectivity.

Available Cyber Backup Target Cyber Security Features

All the backup targets evaluated offer cyber secure capabilities, though the availability, breadth, and implementation of these features vary.

Data Immutability

Data immutability, or storing data in an unchangeable format, represents one feature nearly every backup target supports. When enabled, this feature prevents ransomware attacks from either deleting or encrypting backups stored on the backup target.

Encryption

Encryption represents another backup target feature that has seen an uptick in adoption. Many backup targets have offered at-rest encryption for years. However, few organizations used it due to the overhead it incurs while encrypting or decrypting backups.

This organizational mindset toward using at-rest encryption has since changed. Many ransomware strains attempt to exfiltrate data as part of their attack. Admittedly, encrypting backups does not prevent ransomware from exfiltrating them outside of the organization. However, hackers will find it almost impossible to decrypt and read any encrypted backups they obtain.

Multi-factor Authentication

Using multi-factor authentication (MFA) to log into a cyber secure backup target represents perhaps the most significant enhancement in recent years. Implementing MFA helps ensure only the appropriate administrators access and manage the NAS backup target.

Some backup targets even require a second administrator to authenticate before it allows certain configuration changes. These may include tasks such as changing folder permissions or deleting data, among others.

HA has become relevant due to the role that backup targets play in helping enterprises recover from a ransomware attack.

High Availability

High availability (HA) also appears as a cyber security enhancement with more backup targets offering highly available controller configurations. Organizations may not normally view HA in the context of cyber security. However, HA has become relevant due to the role that backup targets play in helping organizations recover from a ransomware attack.

During restores and recoveries, backup targets may have to perform the following tasks, which include:

- Scanning backups to be used for restores and recoveries for the presence of ransomware.
- Providing fast response times for instant restores.
- Hosting recovered applications and/or data.
- Continuing to serve as a backup target for those parts of the organizations unaffected by ransomware and still operating normally.
- Retrieving backups from the cloud or offsite locations.

Using backup targets that offer HA better equips them to simultaneously perform some or all these tasks. They give organizations the extra raw resources (computing, memory, and networking) that they need at these times.

Artificial intelligence

Artificial intelligence (AI) has yet to make significant inroads as a cyber secure feature on most backup targets. This slow adoption of AI in backup targets somewhat stems from other trends already in play.

For instance, more enterprise backup software has implemented AI to detect ransomware in backups. This development has somewhat negated the need for backup targets to include AI that detects ransomware.

Rather, organizations will primarily find AI in backup targets in its first iteration, machine learning (ML). Currently backup targets may use ML for improved technical support and performing proactive maintenance on their systems. DCIG anticipates through their use of ML to perform these tasks that backup targets will soon offer more sophisticated AI functionality.

The 2PB Cyber Secure Backup Target Dividing Line

All 100+ evaluated backup targets that DCIG evaluated do not necessarily compete against one another. Some offer only block (FC and iSCSI) interfaces. Others offer only NAS (CIFS and NFS) interfaces. Still others offer only object (S3) interfaces.

Additionally, some support various combinations of these storage protocols. Some offer unified storage (block and file.) Some support universal storage (block, file, and object.) Still others provide file and object storage.

DCIG opted to solely focus this report on cyber secure backup targets that minimally supported NAS interfaces. While these backup targets may also offer block and/or object interfaces, DCIG only examined their NAS capabilities.

Backup targets using file protocols offer the greatest flexibility when it comes to ease of management, deployment, and backup operations. However, these characteristics tend to make them more vulnerable to ransomware attacks.

Continued

Sub-2PB+ Cyber Secure Backup Targets // Global Edition

Ransomware increasingly seeks out and discovers file shares presented by backup targets on enterprise networks.

Ransomware often seeks out and discovers file shares presented by backup targets on organizational networks. Once discovered, ransomware may attempt to exfiltrate, encrypt, and/or delete backups on these file shares. It may even try to access the backup target itself and gain control of it. These factors contribute to the need for organizations to select backup targets that offer cyber security features.

Over 90 percent of the 100+ storage systems evaluated by DCIG offered a file system interface. DCIG eliminated those storage systems not positioned as backup targets or lacking appropriate cyber security features. Of those backup targets remaining, two petabytes (PB) of raw storage capacity emerged as a natural dividing line between them.

DCIG did view the remaining cyber secure backup targets with NAS as solutions appropriate for organizations. However, the sub-2PB and 2PB+ dividing line best reflects which backup target models typically compete against one another.

Common Features Across All Sub-2PB Cyber Secure Backup Targets

DCIG evaluated over 100 different storage systems of which thirteen met DCIG's criteria for a sub-2PB cyber secure backup target. Across these thirteen backup targets, DCIG evaluated over 170 features on each one. Despite all these solutions scaling to at least 250TB and no more than 2PB raw storage capacity, organizations may only safely assume that each one minimally possesses the following features:

1. ***Six (6) Ethernet ports.*** Since each backup target supports file networking protocols, organizations would expect each one to support Ethernet connectivity. Further, organizations might expect each solution to offer numerous Ethernet ports due to the amount of raw capacity supported. Yet organizations may only safely assume any one of these backup targets supports six ports.

   Even that number of ports comes with a caveat. Many of the sub-2PB backup targets that offer HA offer controllers in an Active-Passive configuration. In this configuration organizations may only routinely use the Ethernet ports on the Active controller. The remaining ports on the Passive controller remain in standby mode until that controller becomes the Active controller.

2. ***Can minimally provide eight terabytes per rack unit.*** Organizations concerned about the utilization of data center floor space need to pay attention to this metric. Sub-2PB cyber secure backup targets vary widely in their storage density with one model only offering 8 terabytes per rack unit (TB/RU). Another 30 percent support less than 50 TB/RU. On the positive side, five models achieve over 100 TB/RU.

3. ***Compression.*** Due to more storage systems repositioning themselves as backup targets, organizations must verify their data reduction capabilities. With respect to this functionality, organizations may now only assume that all these backup targets offer compression. If they need the solution to deliver deduplication, they should check further. Only slightly more than 65 percent offer deduplication as a core or optional feature.

4. ***NFS/SMB.*** As a report that focuses on backup targets that offer file protocol support, one may assume they support either NFS or SMB. That assumption would be correct. Further, every sub-2PB backup target supports both file protocols. However, not every sub-2PB backup target supports the most secure versions of both protocols.

NFSv3 represents the most widely supported secure file protocol across these backups targets as over 90 percent support it. 84 percent also support the SMBv3 protocol. Organizations should also verify if the backup target supports SMBv1, as nearly 70 percent do. This may present a security risk as SMBv1 represents a known ransomware attack surface. If enabled and used on the backup target, this could present an internal cyber security risk.

5. ***Command line interface.*** Backup targets offer as many as 15 or more ways for organizations to manage them. In the case of sub-2PB backup targets, organizations may only safely assume they can use a command line interface (CLI) to manage one. However, organizations may also manage over 90 percent of sub-2PB backup targets using a web interface.
6. ***High levels of technical support.*** Every provider of sub-2PB cyber secure backup targets offers the option to obtain technical support with 4-hour response times. They may get access to technical support using either email or phone.

SMBv1 represents a known ransomware attack surface and yet is supported by nearly 70 percent of sub-2PB cyber secure backup targets. Organizations should verify they have the option to disable this protocol.

Similarities between the TOP 5 Sub-2PB Cyber Secure Backup Targets

In addition to supporting all the features listed above, each of the TOP 5 sub-2PB cyber secure backup targets also support the following additional features. These include:

- ***Active Directory (AD)/LDAP support.*** While all 2PB+ cyber secure backup targets support AD and LDAP, this does not hold true on all thirteen sub-2PB backup targets. However, each TOP 5 sub-2PB backup target integrates with AD and LDAP.
- ***At-rest data encryption.*** Encrypting data stored at-rest minimizes the possibility that backups, if exfiltrated during a ransomware attack, can be read. Each TOP 5 backup data offers one or more options to encrypt data at-rest.
- ***Highly available configuration.*** Each TOP 5 sub-2PB cyber secure backup target includes a configuration option for two or more controllers to provide HA. However, they do differ in how their respective HA configuration options. One uses an active-active HA configuration, two use an active-passive configuration, and the other two offer a scale-out configuration.
- ***Multi-factor authentication (MFA).*** Securing administrative and user access to the backup target itself has become a priority. As part of a ransomware attack, hackers may attempt to log into the backup target and disable or reconfigure it. MFA helps prevent hackers from ever accessing the backup target. Each TOP 5 backup target supports MFA.
- ***NFSv3.*** Organizations remain hyper concerned about all data in their environment whether at-rest or in-transit. Sending or restoring backups using NFSv3 provides an extra level of security as it offers support for end-to-end encryption. Each TOP 5 sub-2PB cyber secure backup target supports this network file protocol.
- ***Periodic asynchronous replication.*** Copying backups stored on the backup target to another backup target on-site or offsite provides air gapped data protection. Each TOP 5 backup target offers periodic, asynchronous replication to accomplish this task.
- ***Scale to at least 16 Ethernet ports.*** The more front-end Ethernet ports that a backup target offers, the more backup and recovery streams that it can potentially handle. Each of these backup targets scales to at least 16 Ethernet ports in its largest configuration. However, two TOP 5 backup targets use Active-Passive controller configurations. As a result, organizations may only use half of these available Ethernet ports at any one time.

- ***Scale to at least 20 CPU cores.*** Having multiple CPU cores on the backup target helps improve performance during backups, restores, and other tasks such as encryption and replication. Each TOP 5 backup target scales to offer at least 20 CPU cores in its largest configuration.
- ***Web-based management console.*** Each TOP 5 backup target offers a web-based console that organizations may use to access and manage it.

Differences in the TOP 5 backup targets appear in core features such as backup data optimization network protocols, data immutability, and HA.

Differences between the TOP 5 Sub-2PB Cyber Secure Backup Targets

The TOP 5 sub-2PB cyber secure backup targets also differ in how they implement specific features. These differences appear in core features such as backup data optimization network protocols, data immutability, and HA. While organizations may expect backup targets to support these functions, and they largely do, they do implement them differently. Consider:

- ***Backup data optimization network protocols.*** Many organizations have become accustomed to using one or more of the available backup data optimization network protocols.

  These protocols, supplied by both backup software and backup target providers, may compress and deduplicate backups before sending them to the backup target. Alternatively, or additionally, they may facilitate sending multiple backup jobs at the same time. They may also modify file network protocols so they can send larger packets of data.

  For any of these protocols to work, the backup target often must communicate with the backup software. The backup software will let the backup target know it plans to transmit and retrieve the backup data using this protocol. These protocols can significantly reduce backup traffic over the network while also expediting backups and recoveries.

  The level of support that sub-2PB cyber secure backup targets offer for backup data optimization network protocols varies significantly. One does not support or offer any at all. A few backup targets support multiple data optimization network protocols available from numerous backup software providers. One backup target provider offers its own.
- ***Data immutability.*** Data immutability has emerged as a core feature as ransomware attacks often attempt to delete or encrypt backups on backup targets. Storing backups in an immutable data format prevents ransomware from changing, deleting, or encrypting backups.

  Each TOP 5 backup target offers one or options to store data in an immutable format. However, each one implements this feature differently. Some use immutable object storage. Some provide a write once, read many (WORM) option as part of their file system. Some connect to cloud object storage and use its object lock feature. Some even offer the option to use different types of data immutability. Some offer all these options. Organizations should clearly understand how they want to implement data immutability in their environment before selecting a solution or using this feature.
- ***HA configurations.*** Every TOP 5 sub-2B cyber secure backup target offers an HA configuration. However, organizations will find that each one implements HAs differently with three different storage controller configurations across the TOP 5 backup targets. These include active-active, active-standby, and scale-out configurations. Further, four of the five TOP 5 backup targets offer an option with a single controller configuration.

  While each storage controller configuration provides HA, benefits and drawbacks exist with each one. For instance, the Active-Active and Active-Standby architectures represent more established storage controller architectures. They facilitate scaling up storage

capacity. However, they provide limited or no options to add more CPUs, networking ports, or memory to the two controllers. Organizations may also need to migrate data off the backup target once it reaches the end of its life.

- A scale-out architecture provides more flexibility for organizations to incrementally add computing, memory, networking ports and storage. In this way organizations may scale out their backup target as they need. Further, scale-out architectures facilitate updates of specific nodes without needing to replace the entire backup target. However, organizations may find that adding more storage capacity also requires more computing, memory, and networking ports. In some cases, they may not need those extra resources.

TOP 5 Sub-2PB Cyber Secure Backup Target Solution Profiles

Each of the following TOP 5 sub-2PB cyber secure backup target solution profiles highlight at least three ways each solution differentiates itself. These differentiators represent some of the best methods that sub-2PB cyber secure backup targets offer to back up, restore, and/or secure data stored on them. Within each solution, organizations may find features that may better meet their specific needs.

ExaGrid EX18

ExaGrid only uses HDDs in its backup targets that can deliver higher performance than even SSD-based backup targets.

ExaGrid distinguishes itself as being the only TOP 5 provider to focus exclusively on delivering and optimizing backup targets. It delivers the EX18 as a scale out solution that offers the option to start with a single appliance. It may then scale up to 32 appliances in a single logical configuration.

Each EX18 contains 48 TB raw storage that when fully scaled out offers about 1.5PB of raw capacity (~1.1PB usable.) When fully configured, organizations may obtain up to 115 TB/hour of backup throughput.

ExaGrid minimizes or eliminates the need for organizations to perform forklift upgrades of the EX18. Organizations may mix and match any age or size appliance from ExaGrid's seven different Tiered Backup Storage models in the same scale-out system. This mix spans older and newer models so organizations may upgrade and deploy only the amount of storage needed.

Other features that the ExaGrid EX18 offers that further help differentiate it from other TOP 5 sub-2PB cyber secure backup targets include:

- ***Concurrently utilizes multiple features for backup acceleration.*** ExaGrid represents one of the few providers that only uses HDDs in its backup targets. To deliver higher performance than even SSD-based backup targets, ExaGrid minimally uses the following three different techniques:
    1. It optimizes its file system for ingesting large file backup jobs.
    2. Uses job concurrency for parallel backups including integrations with the backup application for front-end load balancing.
    3. It offers a disk-cache Landing Zone so backups complete uninterrupted. Its global deduplication only begins after backup writes complete.
- ***Creates a tiered air gap with a delayed delete policy.*** ExaGrid recognizes ransomware may attack backups stored on its Landing Zone. To protect these backups, ExaGrid takes the following two steps.

First, as backup writes complete, ExaGrid immediately copies, deduplicates, and stores data on a non-network facing, air-gapped Repository Tier. Stored in an immutable format, ransomware can then neither access nor change data stored on this tier.

Second, it offers a configurable delayed delete policy. Backup targets themselves have become susceptible to ransomware attacks with bad actors attempting to log into devices. Implementing the delayed delete policy prevents backups from being deleted even should a hacker take control of an ExaGrid system. Any commands issued to delete data must wait the time specified in the delayed delete policy before a deletion occurs.

- ***Assigns level 2 senior support engineers to each customer account.*** Backup challenges inevitably emerge in every organization. To help quickly resolve them, ExaGrid assigns a level 2 senior support engineer to each customer account. This helps engineers become familiar with the customer's backup environment and its history. Customers may contact their assigned engineer directly to receive support without waiting on a support line or in a ticketing system. ExaGrid has support engineers located around the world.

Arcserve OneXafe 4512

OneXafe automatically stores any backup data in an immutable format.

Arcserve as a company distinguishes itself with a focus on data protection solutions for small and midsize enterprises (SMEs.) The OneXafe 4500 aligns well with Arcserve's overall data protection strategy. While any backup software may use OneXafe, Arcserve Unified Data Protection (UDP) backup software already integrates with OneXafe.

Through this integration with UDP, organizations may choose from different compression, deduplication, and encryption features available on each product. The two products then work together to optimize these settings to achieve better data storage and performance results.

Cyber secure features that the ArcServe OneXafe 4512 offers that help differentiate it from other TOP 5 sub-2PB cyber secure backup targets include:

- ***Built atop an underlying object-based storage system.*** The OneXafe 4512 presents a standard file system interface using common CIFS and NFS protocols accessible by any backup software. However, this file system overlays object-based storage. This equips OneXafe to automatically store any backup data in an immutable format.

  OneXafe delivers on this ideal by only writing data as objects once and then never modifying them. OneXafe then encrypts each object and protects it with a cryptographic hash.If existing backups do get overwritten or changed, OneXafe creates new objects while preserving the existing ones.[3]

- ***Scale-out file system***. Arcserve offers three OneXafe models ranging in capacity from 96 to 216TB in raw capacity. These various capacities position organizations to start with a single OneXafe with only the capacity they need. However, backups can grow quickly which may necessitate adding OneXafe models that offer more capacity and performance.

  OneXafe's scale-out file system makes this proces a straight forward task. Each time an organization introduces a new model, or node, it can add it to the existing OneXafe cluster. The OneXafe scale-out file system then automatically balances the data between the nodes in the new cluster. It performs this task without configurations changes or application downtime.

- ***Includes continuous data protection.*** Organizations may use OneXafe as either a backup target or a general-purpose file server. Regardless of how they use it, OneXafe performs continuous data protection (CDP) by continuously taking immutable

snapshots across the entire. For newly stored data, it takes a snapshot every 90 seconds for the first hour. After that, it takes hourly, daily, and monthly snapshots. This gives organizations multiple recovery points from which to choose for restores in the event of a ransomware attack.[4]

Organizations may centralize and automate the isolation of their backups using Dell's separately licensable PowerProtect Cyber Recovery software.

Dell PowerProtect DD6900

The Dell PowerProtect DD6900 represents the modern iteration of one of the original disk-based backup targets. In its early releases, PowerProtect (formerly Data Domain) focused on delivering high deduplication ratios and backup throughput rates. These factors led to it becoming a widely adopted purpose-built backup target used by many organizations.

While these attributes persist, Dell has in recent years added more optional cyber security features to better address ransomware's threat. For instance, organizations may obtain the DD6900 as a highly available solution with two controllers in an active-standby configuration.[5]

Other features that the Dell PowerProtect DD6900 offers that further help differentiate it from other TOP 5 sub-2PB cyber secure backup targets include:

- ***Two data immutability options.*** Organizations may implement data immutability on the DD6900 by licensing one or both of its two optional Retention Lock features. The Governance Retention Lock option permits DD6900 to lock backups so no user may change or delete them. However, using this option, individuals with administrative privileges may still alter file permissions. If changed, one may then again modify or delete backups.

  The DD6900's more stringent Compliance Retention Lock license prevents even administrators from making any changes or deletions to backup. Once set, no one may change or delete backups until after the expiration of the preset backup date.[6]
- ***PowerProtect Cyber Recovery.*** Organizations may centralize and automate the isolation of their backups using Dell's separately licensable PowerProtect Cyber Recovery software. Cyber Recovery specifically relies upon the PowerProtect DD6900's replication and Retention Lock features to isolate, secure, and restore backups. It may store and secure backups on-premises, at another location, or in AWS, Azure, or Google Cloud.[7]
- ***Detects ransomware in backups.*** Organizations that use Dell's PowerProtect Cyber Recovery solution also gain access to CyberSense. CyberSense performs full content indexing of backups once they are vaulted. It also utilizes machine learning to analyze content-based statistics and detect signs of corruption potentially caused by ransomware. Should a ransomware event occur, CyberSense can provide post-attack forensic reports. They help organizations grasp the breadth and depth of the attack and identify potentially good backups to use for restores.[8]

Huawei OceanProtect X6000

Huawei distinguishes itself by being the only provider to develop and manufacture all software and hardware in all its solutions. Huawei adopted this approach for multiple reasons. Using the same software across all its backup, cloud, and storage solutions provides the same management experience across them. This then positioned Huawei to make ransomware protection capabilities available across all its solutions.

On the hardware side, Huawei delivers high levels of availability in each of its backup solutions. The Huawei OceanProtect X6000 illustrates this capability. It represents the only sub-2PB cyber secure backup target to offer active-active storage controllers with both all-flash and all-HDD models. In this configuration, both controllers simultaneously access all backend storage to provide high availability and performance.

The Huawei OceanProtect X6000 represents the only sub-2PB cyber secure backup target to offer active-active storage controllers with both all-flash and all-HDD models.

Cyber secure features that the Huawei OceanProtect X6000 offers that help differentiate it from other TOP 5 sub-2PB cyber secure backup targets include:

- ***Air gap replication and ransomware checks.*** Using the OceanProtect X6000 organizations may configure a replication Service Level Agreement (SLA). This setting determines the replication frequency and when the network link becomes active.

  The OceanProtect first makes copies of backups in the form of read-only snapshots on the primary OceanProtect X6000 target. Once created, the Air Gap network link goes live. It then replicates the snapshots from the primary backup target to the X6000 in the isolation environment. The network link then gets turned off.

  Once off, the X6000 in the air gapped environment encrypts the replicated snapshots and checks them for ransomware. If it does not detect any ransomware, it applies compliance WORM attributes to the snapshots to prevent data tampering.
- ***End-to-end data encryption.*** To counter the growing problem of data leakage, or exfiltration, during ransomware attacks, the OceanProtect X6000 offers end-to-end (E2E) data encryption. It encrypts data at-rest using AES-256 array-based encryption. Organizations may choose from SMBv3, NFSv4.0, or NFSv4.1 encryption to replicate data in-flight during air gap and remote replication. The OceanProtect X6000 accounts for encryption's overhead with its many multi-core CPUs.
- ***Scan backups for ransomware by connecting to its OceanCyber data security appliance.*** Despite all the precautions that organizations take to protect their data from ransomware, ransomware may still slip in undetected. This may occur due to new strains coming in undetected by current organizational anti-malware and firewall software. To counter this, Huawei also offers its OceanCyber data security appliance for more holistic data protection.

  The OceanCyber data security appliance connects to multiple Huawei storage systems, including the OceanProtect X6000. Using OceanCyber appliances, organizations may set and manage security policies to monitor and alert for ransomware across these systems. It can scan data at up to 50 TiB/hour for ransomware and generate alerts if it detects any anomalies.[9]

iXsystems TrueNAS X20

iXsystems represents one of multiple storage providers that has for years offered cost-effective storage systems used as backup targets. iXsystems offers the choice of TrueNAS on either FreeBSD or Debian Linux, both Open Source operating systems, and their OpenZFS file system. Using this approach iXsystems has steadily increased the number of relevant backup target software features on them.

For instance, the TrueNAS X20 includes many of the software features often associated with a backup target. These include compression, deduplication, snapshots, replication, and even read and write acceleration. iXsystems' approach to software development has resulted in the price of TrueNAS X20 remaining attractive, starting as low as $12,000.[10] However, organizations that need dual controller or higher levels of support should expect to pay more.

Cyber secure features that the iXsystems TrueNAS X20 offers that help differentiate it from other TOP 5 sub-2PB cyber secure backup targets include:

- ***Built-in data immutability.*** Using OpenZFS as its underlying file system grants the TrueNAS X20 access to built-in data immutability. Anytime data gets changed or overwritten, TrueNAS automatically retains any blocks containing old data. This is known as copy-on-write. Using this feature, should ransomware attack data on the X20, organizations may roll back to prior backups.

The TrueNAS X20 Cloud Sync feature equips organizations to replicate data to cloud storage from over 15 supported cloud providers.

The X20's snapshot feature capitalizes on the inherent copy-on-write feature by taking read-only snapshots. Each snapshot records all the data and metadata blocks that comprise the file system at the time of the snapshot.

- ***Offers multiple encryption options.*** Data leakage represents one of the bigger threats that any ransomware event presents to organizations. To mitigate the impact of any data leakage, the TrueNAS X20 can encrypt data both at-rest and in-flight.

  Organizations may order X20 models with self-encrypting drives, either SSDs or HDDs. This option minimizes the possibility of data leakage in the event of hardware theft or compromise. They may also encrypt data at-rest using the TrueNAS X20's OpenZFS. It encrypts block, file, and object data at-rest. Finally, organizations may use TrueNAS to encrypt data-in-flight, such as when they replicate data between TrueNAS systems.[11]
- ***Can synchronize data with multiple cloud providers.*** Moving data offsite to the cloud creates an air gap that further helps protect organizational data from ransomware attacks. Storing data on cloud object storage with object lock enabled also provides another layer of data protection. The TrueNAS X20 Cloud Sync feature equips organizations to perform this task.

  Included with TrueNAS, Cloud Sync can replicate data to cloud storage from the over 15 different providers it supports. TrueNAS can both transfer data to (push) or transfer data from (pull) any of the supported cloud providers. Many organizations will configure Cloud Sync to push backups to the cloud on a regular schedule. However, if they need to restore, they can access that same task, expand it, and click on Restore to pull data back.[12]

Sub-2PB Cyber Secure Backup Target Inclusion Criteria

- Offers cyber security features to protect itself and data stored on it.
- Scales to at least 250TB and to no more than two petabytes of raw storage capacity.
- Ships as a physical appliance.
- Shipping and available by March 1, 2024.
- Sufficient information available for DCIG to make an informed, defensible decision.

DCIG Disclosures

Providers of some of the sub-2PB cyber secure backup targets covered in this TOP 5 report are or have been DCIG clients. This is not to imply that their solution was given preferential treatment in this report. In that vein, there are some important facts to keep in mind when considering the information contained in this TOP 5 report:

- No provider paid DCIG a fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any provider that its solution would be included in this TOP 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a TOP 5 designation.
- All research is based upon publicly available information, information shared by the provider, and the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the features worked as described.

- No negative inferences should be made against any provider or solution not covered in this TOP 5 report.
- It is a misuse of this TOP 5 report to compare solutions included in this report against solutions not included in it.

No provider was privy to how DCIG weighted individual features. In every case the provider only found out the rankings of its solution after DCIG's analysis was complete. To arrive at the TOP 5 solutions included in this report, DCIG went through a seven-step process to come to the most objective conclusions possible.

1. DCIG established which features would be evaluated.
2. The features were grouped into five general categories.
3. DCIG weighted each feature to establish a scoring rubric.
4. DCIG identified solutions that met DCIG's definition for a sub-2PB cyber secure backup target.
5. A survey was completed for a model of each evaluated backup target.
6. DCIG evaluated each backup target based on information gathered in its survey.
7. Solutions were ranked using standard scoring techniques. ■

1. https://www.blackfog.com/the-state-of-ransomware-in-2023/. Referenced 1/8/2024.
2. Ibid.
3. https://documentation.arcserve.com/Arcserve-UDP/Available/9.0/ENU/Bookshelf_Files/PDF/AD210071.pdf. Referenced 3/15/2024.
4. Ibid.
5. https://www.dell.com/support/manuals/en-us/dd-os-7.7/dd_p_7.x_spec_guide/dd6900?guid=guid-23d93de3-37f6-4ee3-a509-cdb7a5eba4a9&lang=en-us. Referenced 3/16/2024.
6. https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq. Referenced 3/16/2024.
7. https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf. Referenced 3/16/2024.
8. Ibid.
9. https://e.huawei.com/id/products/storage/oceanprotect/oceancyber-series. Referenced 1/26/2024.
10. https://www.truenas.com/x-series/?__hstc=216824393.aebc7f92506508fca504afa07bd8bbed.1709218706849.1709218706849.1710686693262.2&__hssc=216824393.1.1710686693262&__hsfp=1663256162&_gl=1*47769u*_gcl_au*MTcwNTAzOTc3OS4xNzA5MjE4NzA0. Referenced 3/17/2024.
11. https://www.truenas.com/solution-guides/?__hstc=216824393.aebc7f92506508fca504afa07bd8bbed.1709218706849.1710686693262.1710689234365.3&__hssc=216824393.1.1710689234365&__hsfp=1663256162&_gl=1*1fom00b*_gcl_au*MTcwNTAzOTc3OS4xNzA5MjE4NzA0#TrueNAS-PDF-solution-brief-truenas-privacy-and-security-compliance-features/1/. Referenced 3/17/2024.
12. https://www.truenas.com/docs/core/coretutorials/tasks/creatingcloudsynctasks/. Referenced 3/17/2024.